DISKCRYPT MOBILE

DCM300

USER MANUAL

This page has been left blank intentionally

ST Electronics (Info-Security)

ST Electronics
A company of ST Engineering

DiskCrypt® *Mobile*

USER MANUAL

G-P6019-TM001
(ISSUE A)

Issue Date: Apr 2009

Copyright
© 2009 ST Electronics (Info-Security) Pte Ltd. All rights reserved. No part of this material may be reproduced, transcribed, used or disclosed to any third party in any form or by any means, without the written permission of ST Electronics (Info-Security) Pte Ltd.

Trademarks
DigiSAFE logo and DiskCrypt are either trademarks or registered trademarks of ST Electronics (Info-Security) Pte Ltd in Singapore and/or in other countries. DigiSAFE logo is a registered trademark in U.S. Patent and Trademark Office. All other trademarks or registered trademarks are the property of their respective owners.

2009.04.01 Version 1.0

ST Electronics (Info-Security) Pte Ltd
ST Electronics Jurong East Building
100 Jurong East Street 21
Singapore 609602
Tel: (65) 6568 7118
Fax: (65) 6568 7226
Email: info@digisafe.com
Website: www.digisafe.com

This page has been left blank intentionally

Disclaimer

DigiSAFE DiskCrypt *Mobil*e DCM300 has been designed to be compliant with the SATA hard drive operating specifications as well as USB 1.1/2.0 and Firewire 400/800 operating specifications.

ST Electronics (Info-Security) accepts no liability for any loss of data or the inability of DiskCrypt *Mobile* to work with equipment that are not compatible with the above operating specifications. Nor can ST Electronics (Info-Security) accept any liability or responsibility for software which is also non compliant.

Thank you for purchasing DiskCrypt *Mobile*.

Contents

1. About this Guide 1

2. Introduction 2

2.1. About DiskCrypt *Mobile* DCM300 2
2.2. DCM300 Connection Ports 3
2.3. Checklist 3
2.4. Specifications 4

3. Installation 5

3.1 Installing a hard drive 5
3.2 Connecting DCM300 to a computer 6
3.3 Using the built-in keypad 7
3.4 Using an AC Power Adapter 8

4 Authentication 9

4.1 Inserting the smart card 9
4.2 Entering your PIN 9

5 Setting up the drive 10

5.1 Setting up a new drive 10
5.2 Setting up an existing drive 10

6 Disconnecting DCM300 11

7 Smart Card Security Features 12

7.1 PIN Change 12
7.2 Administrative Mode 13

8 Helpful Information 14

8.1 Partitioning and formatting your hard drive 14

9 Care and Handling 15

10 Frequently Asked Questions 16

11 Troubleshooting 19

AMENDMENT RECORD

AMDT NO.	AFFECTED PAGE(S)	ECN/DCR NO.	EFFECTIVE DATE

1. About this Guide

This guide is designed to provide step-by-step instructions for installation of DigiSAFE DiskCrypt *Mobile* DCM300 and as a reference for its operation and usage.

PLEASE READ AND FOLLOW THE INSTRUCTIONS PROVIDED IN THIS GUIDE CAREFULLY AND THOROUGHLY.
FAILURE TO DO SO MAY RESULT IN DAMAGE TO DISKCRYPT MOBILE AND ANY OR ALL OF THE CONNECTED DEVICES.

2. Introduction

2.1. About DiskCrypt *Mobile* DCM300

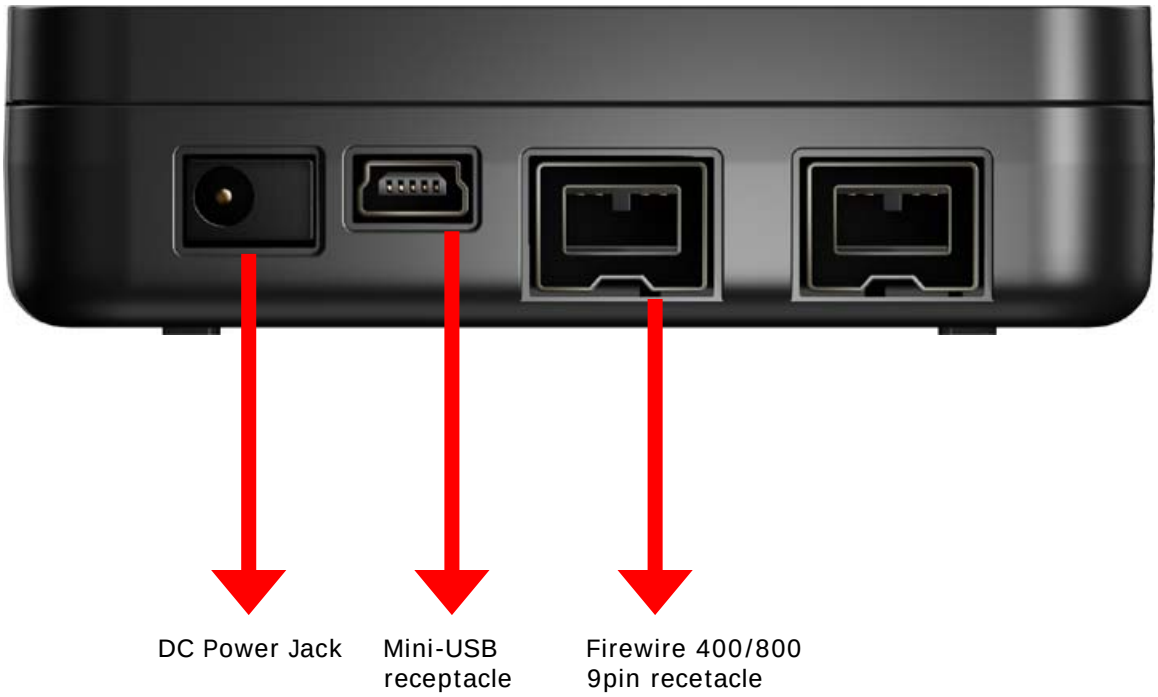
Congratulations on your purchase of DigiSAFE DiskCrypt *Mobile* DCM300. DiskCrypt *Mobile* DCM300 represents the most advanced secure Mobile storage solution today, utilizing smart card authentication technology and AES 128/256 bits full disk encryption. With DiskCrypt *Mobile*, you can enjoy Mobile storage with the speed and convenience of both USB 2.0 and Firewire 400/800 in a compact form factor, and be assured that your data is safe from prying eyes.

DCM300 is a secure portable hard drive enclosure consisting of a 2.5" SATA hard drive enclosure and a hardware-based encryption module that performs full disk encryption, i.e. it encrypts every byte and every sector of data that is written into the hard drive. The device is designed to fit standard 2.5" hard drives with a SATA interface, and communicates with the computer via either standard USB 2.0 ports or Firewire 400/800 ports. By encrypting every single byte and sector, DCM300 is operating system independent and does not require any software drivers. It also encrypts all temporary files, as well as areas that would normally be missed and left "in the clear" by software encryption products. Encryption and decryption occurs transparently without any loss in disk performance. Users simply use their computers as usual with the assurance and complete piece of mind that their data is fully protected in the unfortunate event that their hard drives are stolen or lost.

DCM300 stores the hard drive encryption key in smart cards (two are provided per unit). Smart card technology is well understood and represents the highest level of security possible for secure data storage. It is vastly more secure than other solutions that use hardware tokens, where the encryption key is stored in insecure memory that can be easily duplicated. In contrast, smart cards store the encryption key securely within, and can only be accessed upon presentation of a valid PIN. The user will need both the smart card as well as knowledge of its PIN to be able to access the data in the connected hard drive. By doing so, DCM300 enforces two-factor authentication, which is a higher security protection by ensuring that the user possesses both the physical Smart Card and the knowledge of its PIN.

The user is required to authenticate him or herself each time DCM300 is plugged into the computer. After authentication, the drive presents itself to the operating system and the user is granted normal drive access.

2.2. DCM300 Connection Ports



2.3. Checklist

The following items are included with DiskCrypt *Mobile* DCM300. If you discover any missing items, please contact your distributor/retailer.

- 1 x DigiSAFE DiskCrypt *Mobile* DCM300
- 1 x USB Y cable
- 2 x DiskCrypt *Mobile* smart cards
- 1 x black pouch

2.4. Specifications

Drive compatibility	• 2.5” SATA 9.5mm height drives (any capacity)
Bus Interface	• USB 2.0 • Firewire 400/800
Physical	• SATA 22 pin connector • USB mini-B receptacle • Firewire 9-pin receptacle • 1.3mm 5VDC jack • Smart Card slot • Dimensions: 130mm (L) x 78mm (W) x 22mm (H)
Power	• Approx 5V 400mA max (excluding power drawn by the HDD)
Authentication	• Supports two-factor authentication via smart card and PIN
Smart Card	• Supports ISO-7816 T=0 Class B cards
Encryption	• NIST[1] certified AES hardware cipher engine • Supported key strength: 128-bits/256-bits
Key Management	• User-configurable PIN • Admin password for administrative mode
Certifications and Standards	• Designed to meet FIPS 140-2 Level 2 • FCC, CE • RoHS compliant
Operating Systems	• Operating System independent • Tested with Windows® XP, 2000, Mac OS X and Linux

[1] NIST – The National Institute of Standards and Technology of the United States of America

3. Installation

To use DiskCrypt *Mobile* DCM300, simply remove the bottom cover and install your 2.5" SATA hard drive by connecting it to the 22pin SATA connector within. Detailed step-by-step instructions are provided in this section.

DCM300 is not shipped with any hard drive. You may purchase a standard 2.5" SATA hard drive or use your existing 2.5" SATA hard drive with DCM300.

3.1 Installing a hard drive

DiskCrypt *Mobile* DCM300 supports standard 2.5" SATA hard drives. To install your 2.5" hard drive, follow these three easy steps:

1. Turn the DCM300 enclosure over and carefully remove its bottom cover, by pressing the latch that can be found on the sides of the unit.

2. Connect the 2.5" SATA hard drive firmly to the 22pin SATA connector on the tray.

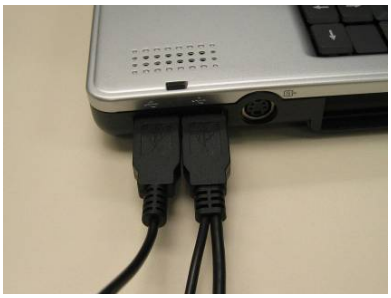
3. Carefully snap the bottom cover to the top cover.

Note:
- *Please ensure the bottom cover is firmly snapped on to the top cover.*

3.2 Connecting DCM300 to a computer

Once your hard drive is installed in DCM300, you are ready to use it with your computer. To do so, follow these easy steps:

1. Insert the USB or Firewire 400/800 connector to your computer's corresponding port.



2. Insert the USB or Firewire 400/800 to DCM300's corresponding port. Ensure correct connector orientation to obtain a snug fit.

3. The unit's backlight will turn on, indicating that DCM300 has powered up.

***Notes on using USB port**:*

- *Do not attempt to use DCM300 when connected to a bus-powered USB hub or USB extension cable.*
- *Connecting to a non-USB compliant port may cause operation damage or failure.*
- *If insufficient power to DCM300, connect both connectors of the USB Y-cable to the computer's USB ports.*
- *To achieve USB 2.0 speeds, always connect DCM300 to a USB 2.0 Hi-Speed port.*

***Notes on using Firewire port**:*

- *If you are using Firewire 400, please ensure that you have a 9-to-6 pin bilingual cable and connect the 6 pin end to the computer's Firewire port.*

3.3 Using the built-in keypad

The built-in keypad allows you to enter/change your PIN (refer to Section 4 on Authentication and Section 7 on changing PIN). It works on the principle of capacitive sensing to provide a better user experience and can detect the presence of a touch on the button.

Note:

- *The keypad works on the principle of touch and users need NOT exert force on a button to register a key pressed.*
- *It is recommended to avoid exerting force on the keypad since doing so over time will cause the buttons to lose their sensitivity.*

3.4 Using an AC Power Adapter

DCM300 is designed to be powered by the USB bus. However, due to variances of your PC's hardware, the host USB power supply may be inadequate at times. In this case, an extra AC power adapter is needed.

The specifications of the power adapter are:
Input: 100-240V AC, 50-60Hz, 0.5A
Output: +5V DC, 2A
DC plug: 1.3mm

Note:

- *The AC Power adapter is not included as part of the packaging items.*
- *Please ensure that you have the right power adapter with you. Using an incorrect power adapter may cause the unit to malfunction.*
- *DCM300 remains in authenticated mode as long as power is supplied. Please ensure that you unplug the AC power adapter when away.*

4 Authentication

DCM300 requires users to authenticate themselves via two-factor authentication before they are granted access to the installed drive. In order to do so, users must have the included smart card (something you have) and its associated PIN (something you know). The authentication process involves inserting the correct smart card into DCM300, followed by PIN entry. Upon completion of these two steps, the connected drive will present itself to the operating system, and can be used like a normal drive.

4.1 Inserting the smart card

DCM300 is shipped with two smart cards. DigiSAFE recommends that you use only one card and keep the other in a secure place. In the event that one card is stolen/lost, you may authenticate with the other card.

To begin authentication, simply insert the smart card with the contacts facing down. You may insert the card before or after connecting DCM300 to your computer. Once a valid card is inserted, the Status LED will blink once. If an invalid card is inserted, the Error LED will light up.

4.2 Entering your PIN

Once DCM300 recognizes that a valid card is inserted, you may proceed to enter your 8-digit PIN. The default factory PIN is **"12345678"**. At the end of your PIN entry, press the **Enter** button.

***Note**:*

- *If an incorrect PIN is entered, the Error LED will blink continuously. Press the **Esc** button to restart DCM300. If you have mistyped your PIN, press the **Esc** key at any time to restart the entire authentication process.*
- *You will be locked out of your smart card after **8 incorrect PIN** attempts. Therefore, after about 5 incorrect attempts, it is advised that you seek for technical assistance as in Section 11.Troubleshooting*

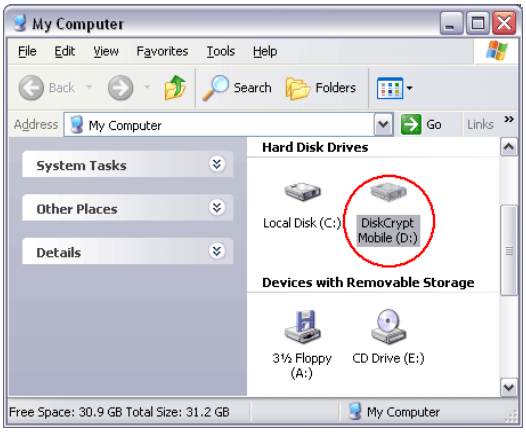
Insert the smart card into the smart card slot with the contacts facing down and the word "DigiSAFE" on the card facing up

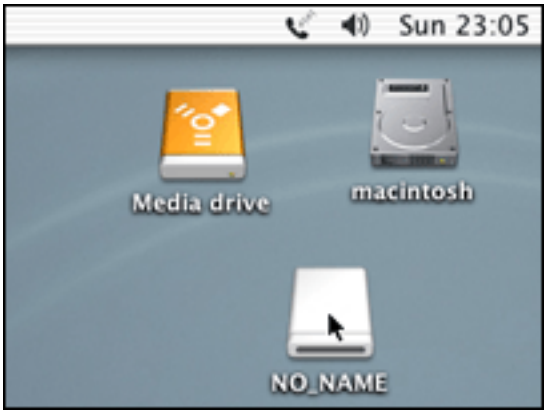
*Enter your 8-digit PIN, followed by the **Enter** button*

5 Setting up the drive

After you have successfully authenticated yourself to DCM300, drive access will be granted. The connected drive will then present itself to the operating system as a removable drive. Please wait for a few seconds for this process to fully complete. The mounting duration depends on your drive and operating system.

Once the drive appears in your operating system, you may proceed to use it like a normal hard drive.





5.1 Setting up a new drive

To set up a new hard drive, you have to partition and format it. Follow your operating system's instructions on how to do so, or refer to Section *8.1 Partitioning and formatting your hard drive*.

5.2 Setting up an existing drive

No additional steps are required to set up a previously formatted hard drive. The drive will be recognized by the operating system and may be accessed as per normal.

Note:

- *When using an existing drive, ensure that the drive's file system is compatible with your Operating System.*
- *DCM300 provides data-at-rest protection. After successful authentication, data in the drive can be access as per normal usage. For maximum security, do not leave DCM300 connected in authenticated mode while you are away from your computer.*
- *As with any other storage solution, please ensure that you make regular backups of your data to protect against possible data loss.*

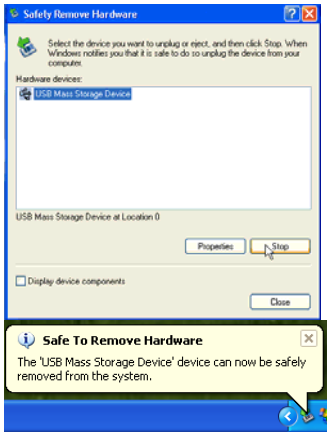
6 Disconnecting DCM300

CAUTION: To prevent data loss, ensure that all active applications are closed before shutting down DCM300.

To disconnect DCM300, follow your operating system's proper device removal process.

Windows XP

1. Double click on the **Safely Remove Hardware Icon** in your system tray.
2. Select **USB Mass Storage Device** from the list, and select the device you would like to remove.
3. Click **Stop**.
4. Click **OK** to confirm drive disconnection.
5. Click **Close**.
6. Windows will inform you that it is safe to disconnect the device.
7. You may now safely disconnect the USB cable from your computer.


Safety Remove Hardware
Select the device you want to unplug or eject, and then click Stop. When Windows notifies you that it is safe to do so unplug the device from your computer.
Hardware devices:
USB Mass Storage Device
USB Mass Storage Device at Location 0
Properties
Stop
Display device components
Close
Safe To Remove Hardware
The 'USB Mass Storage Device' device can now be safely removed from the system.

Mac

1. Locate the **Removable Disk Icon** associated with DCM300.
2. Drag the icon to the **Trash** icon on your desktop and wait for the icon to disappear
3. You may now safely disconnect the USB cable from your computer.

7 Smart Card Security Features

You can perform certain smart card related security functions with DCM300. These functions are only available before/during authentication. The following functions are available.

CAUTION: Smart Card security and administrative functions must be performed carefully as they cause changes in smart cards and associated PINs. Please read the following instructions carefully and follow them when performing administrative functions.

7.1 PIN Change

You can change your smart card PIN with DCM300. It is recommended that you change the default factory PIN to another one that only you know. Follow these steps to change your PIN.

1. Insert smart card into DCM300.
2. Press the **Change Pin** button, followed by the **'1'** button.
3. Press **Enter**. The Status LED will blink three times.
4. Enter the current 8-digit PIN and press **Enter**. The Status LED blinks twice to notify that you may press the new PIN.
5. Enter the new 8-digit PIN and press **Enter**. The Status LED blinks twice to notify that you may press the confirmed new PIN.
6. Enter the new confirmed 8-digit PIN and press **Enter**.

Upon a successful PIN change, DCM300 will proceed to connect the drive. At the same time, the Status LED will blink three times and there will be two 'beep' sounds upon a successful PIN change. If not, the Error LED will blink continuously.

***Note**:*

- *DCM300 only accepts 8-digit PINs. If a shorter or longer PIN is entered, the Error LED will blink continuously. Press the **Esc** button to restart the authentication process again. You will need to restart the entire PIN Change process from step 2.*
- *Pressing the **Esc** key restarts the entire authentication process.*
- *Smart card PINs are specific to the physical smart card. Please be aware that you may have different PINs for each of the two included smart cards.*
- *Again, you will be locked out of your smart card after **8 incorrect PIN** attempts.*

7.2 Administrative Mode

You may enter Administrative mode with DCM300. In this mode, you can change the Admin PIN and/or initialize a DigiSAFE smart card so as to use it with DCM300. Additional DigiSAFE smart cards may be purchased from STEE-InfoSec. You will need a supported DigiSAFE smart card, and knowledge of the Admin PIN to enter the mode. The default factory Admin PIN is "**87654321**". To exit Administrative Mode, reconnect the USB cable.

7.2.1 Smart Card Initialization

To initialize a smart card, follow these steps:

1. Insert new smart card into DCM300.
2. The Error LED will light up indicating an invalid card has been inserted. Ignore the LED.
3. Press the **Admin** button and press **Enter**. The Status LED will blink three times.
4. Enter the 8-digit Admin PIN and press **Enter**. The Status LED will blink three times and there will be two 'beep' sounds if the correct PIN was entered.
5. DCM300 will proceed to initialize the smart card to be used with that particular DCM300 unit.

Note:
- *Once a new smart card is initialized, you will need to repartition/reformat any existing drive, as the encryption key will be different. The existing data in the drive will be unreadable with the new card.*

7.2.2 Change Admin PIN

The Admin PIN provides a layer of protection around your DCM300 unit to deter others from unauthorized usage of your DiskCrypt *Mobile*. It is recommended that you change the default factory Admin PIN to another one that only you know. To change your Admin PIN, follow these steps:

1. Insert the smart card into DCM300.
2. Press the **Change Pin** button, followed by the **'0'** button.
3. Press **Enter**. The Status LED will blink three times.
4. Enter the current 8-digit Admin PIN and press **Enter**. The Status LED blinks twice to notify that you may press the new Admin PIN.
5. Enter the new 8-digit Admin PIN and press **Enter**. The Status LED blinks twice to notify that you may press the confirmed new Admin PIN.
6. Enter the new confirmed 8-digit Admin PIN and press **Enter**.
7. The Status LED will blink three times and there will be two 'beep' sounds if the PIN change is successful.

If you have mistyped your PIN, press the **Esc** key at any time to restart the entire authentication process.

8 Helpful Information

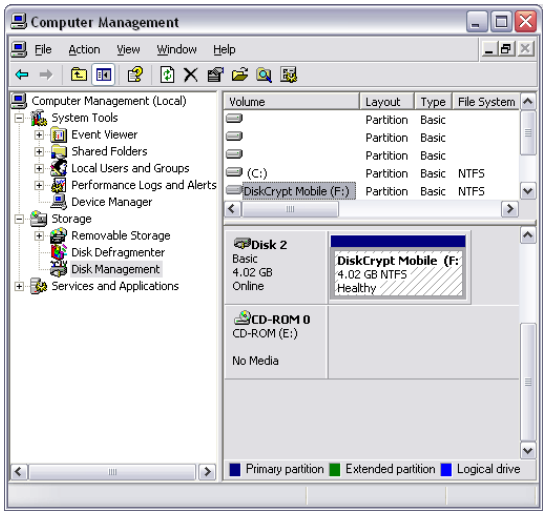
8.1 Partitioning and formatting your hard drive

In order to use a new hard drive with DCM300, you will have to partition and format the drive. Follow these steps to do so:

CAUTION: Performing partition and format operations will erase all data in the drive.

Windows XP

1. Connect and authenticate into DCM300.
2. Right click on **My Computer** and Select **Manage**.
3. From the **Computer Management** window, select **Disk Management**.
4. Right click on the drive and choose **Initialize**.
5. Right click on the drive and select **New Partition**.
6. Follow the New Partition Wizard to create as many partitions as desired.
7. Right click on each partition and select **Format** to format the drive in either FAT32 or NTFS.
8. The drive is ready to be used once formatting completes.

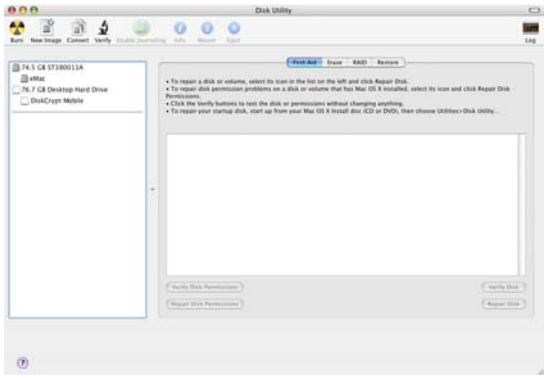


***Note**:*

- *You must have Administrator privileges to use the Disk Management utility.*
- *For drives larger than 137GB, you will need Windows SP3 for Windows 2000 and SP1 for Windows XP.*

Mac

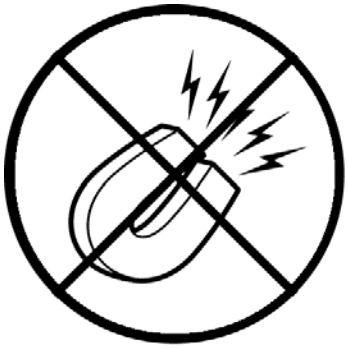
1. Connect and authenticate into DCM300.
2. Enter the **Applications** folder, followed by the **Utilities** folder
3. Run **Disk Utility**.
4. Select DCM300 on the left hand column and click on the **Partition** tab.
5. Choose the number, size and names of the desired partitions.
6. Mac OS will then format the drives automatically.
7. The drive is ready to be used once formatting completes.



9 Care and Handling

The following are some important information on the proper care and handling of DCM300. Please take a moment to review these instructions.

- As with any storage solution, it is recommended that the data of the connected drive be backed up regularly.
- Ensure that you follow the proper removal procedure to disconnect DCM300.
- Do not move or disconnect this device from your computer while it is reading or writing data. This may cause damage to DCM300 and it is possible that the data that is read from or written to the device becomes corrupted.
- Do not place this device near a heat source or expose to direct flame or heat.
- Do not place the device near to equipment generating strong electromagnetic fields. Exposure to strong electromagnetic fields may cause the device to malfunction or data to be corrupted.
- Do not drop or cause shock to your DCM300.
- Do not expose DCM300's internals to water.
- Do not attempt to disassemble and service DCM300 yourself.



10 Frequently Asked Questions

What is DiskCrypt *Mobile* DCM300?

DiskCrypt *Mobile* DCM300 is a secure hard disk enclosure for 2.5" SATA hard drives. It provides access control via two-factor authentication and data-at-rest security via hardware-based full disk encryption.

How easy it is to use DiskCrypt *Mobile* DCM300?

It is very simple and straightforward. After installing the hard drive into DCM300, it is as simply as connecting DCM300 to your computer, inserting your smart card and entering a PIN. No software installation is required at all.

What are the advantages of using DiskCrypt *Mobile* over other USB drive enclosures?

DiskCrypt *Mobile* provides state of the art security via two-factor authentication and hardware-based full disk encryption. It is the only hard disk enclosure that utilizes smart card technology for two-factor authentication[1].

What are the advantages of smart card authentication over hardware keys/tokens?

Smart cards are a proven technology for secure storage of information. DiskCrypt *Mobile* stores the encryption key in smart cards. While other encrypted drive enclosures make use of hardware keys to store the encryption key, these keys are not secure, and can be easily duplicated if they are lost/stolen, hence compromising the encryption key and the data within the hard drive. Smart cards however require a PIN to access data within. Even if the cards and enclosure are both lost or stolen, your data is still secure as the PIN is only known to you.

What is two-factor authentication?

Two-factor authentication is an authentication protocol that requires two independent methods to establish one's identity and privileges. DiskCrypt *Mobile* implements two-factor authentication by requiring that the user have the associated smart card (something you have) and knowledge of the PIN (something you know). This offers stronger security than traditional password or hardware key only security.

What are the advantages of two-factor authentication?

Two-factor authentication offers stronger security than traditional password, biometric or hardware key/token only systems. Should your smart card be stolen/lost along with your DiskCrypt *Mobile*, your data will still be secure as long as the PIN is only known to you.

[1] As of 4/13/2009

What are the advantages of hardware-based full disk encryption over software encryption solutions?

- Unlike existing software solutions, DiskCrypt *Mobile* encrypt every single byte and sector of the hard drive. This means all temporary files, all partitions and even the boot sector is encrypted
- One major disadvantage of existing software disk encryption products is that they are Operating System (mostly Windows) dependent. DiskCrypt *Mobile* is independent of the OS or the host system BIOS and thus support any OS.
- DiskCrypt *Mobile* does not involve any tedious and error-prone software installation and configuration. Just plug DiskCrypt *Mobile* in the computer, authenticate yourself and you are ready to go.
- Once installed, DiskCrypt *Mobile* does not require any maintenance or patches thus reducing the total cost of ownership of the product.
- There are also no performance overheads due to encryption/decryption of data, unlike software-based solutions.

What happens when DiskCrypt *Mobile* malfunctions?

Every DiskCrypt *Mobile* is subjected to a stringent quality assurance process prior to shipment. However, hard drives installed in DiskCrypt *Mobile* still have a limited lifetime. As such, users are advised to backup their data regularly. The encryption key is stored securely in the included smart cards. In the event that DiskCrypt *Mobile* malfunctions, the data in the drive will still be readable as long as the smart cards are present. Simply install your drive in another DiskCrypt *Mobile* of the same encryption key length, initialize your card(s), and you may use the new DiskCrypt *Mobile* as per normal.

Is the boot sector also encrypted?

Yes, DiskCrypt *Mobile* employs full disk encryption (FDE), meaning every single byte and sector of your hard drive is encrypted.

Does encryption decrease drive performance?

No. The on-the-fly hardware encryption engine in DiskCrypt *Mobile* DCM300 is faster than the data transfer rate of the SATA interface, and thus does not incur any performance overhead, nor require any additional CPU resources.

How strong is the encryption of DiskCrypt *Mobile*?

DiskCrypt *Mobile* DCM300 offers AES encryption scheme with a key-strength of either 128 bits or 256 bits.

Can the PIN be changed later without data loss?

Yes, the smart card PIN may be easily changed during the time of authentication without any data loss. Please note that PINs are smart card specific so changing the PIN with one smart card does NOT automatically change the PIN of another.

Can I use DiskCrypt *Mobile* with my operating system?

Yes! Because DiskCrypt *Mobile* uses hardware for the authentication and encryption processes, it is operating system independent. As long as your choice of operating system supports the USB Mass Storage class specification and/or Firewire 400/800 specification, you may use DiskCrypt *Mobile* with it. DiskCrypt *Mobile* has been tested under Windows XP, 2000, Mac OS and Linux.

What happens if I lose my smart card?

The smart cards included contain the encryption key of the installed drive. The key is protected by your PIN, and hence it is inherently secure as long as your PIN is not compromised. If you lose your 1st card, please continue to use the 2nd card to access your drive. You may wish to purchase additional cards, and/or our key management system to duplicate cards. Please note that new cards will come with new encryption keys, so please backup your data with your existing card before using the new cards.

11 Troubleshooting

In the event that your DCM300 does not function properly, please refer to the following checklist to find out what the problem is. If further technical support is required, please contact your DiskCrypt *Mobile* reseller or DigiSAFE Technical Support at

DigiSAFE Technical Support
Email: services@digisafe.com

Problem	Query	Possible reason and remedy
The keypad is inactive	*Is the unit's backlight on?*	Ensure that the USB connector is firmly connected to your computer's USB port. If you are using Firewire, ensure that the Firewire connector is firmly connected to the computer's Firewire port.
	Has a smart card been inserted?	Insert a valid smart card into the DCM300.
	Is the Error LED lighted?	Ensure that a valid card is inserted, and that the card orientation is correct, by inserting the card with the contacts facing down.
Authentication fails	*Is the Error LED lighted?*	Ensure that a valid card is inserted, and that the card orientation is correct, by inserting the card with the contacts facing down.
	Is the Error LED blinking?	A wrong password has been entered. Press the Esc button to restart the authentication process.
The drive is not recognized.	*Does the Status LED stay on all the time?*	Ensure that the USB connector is firmly connected to your computer's USB port. If you are using Firewire, ensure that the Firewire connector is firmly connected to the computer's Firewire port.
	Does the drive's icon appear on the computer?	Check for the drive icon in your operating system. Ensure that the DCM300 is not connected to a bus-powered USB hub or a USB extension cable. If this still doesn't work, an extra power adaptor might be needed.
	Is the hard drive new?	A new drive that has not been previously partitioned and formatted will need to be done so. Refer to 8.1 Partitioning and formatting your hard drive for more information.

Problem	Query	Possible reason and remedy
The drive is not recognized.	*Is the file system supported by the operating system?*	When using an existing drive in a new operating system, ensure that the file system used by the drive is compatible with the new operating system.
	Is your DiskCrypt Mobile DCM300 connected to a USB port?	Ensure that the DCM300 is plugged into a USB port directly rather than an extension cable or hub. If the drive isn't recognized when plugged into the front USB ports, try the rear USB ports.
	Are you using the included DiskCrypt Mobile USB cable?	Only use the included DiskCrypt *Mobile* USB2.0 certified Y-cable. Other USB cables may be of inferior quality.
	Do you hear clicking sounds from your drive?	The drive might be experiencing trouble spinning up due to insufficient power from the USB port(s). Connect both USB connectors directly into your PC's USB ports. Do not connect them to extension cables or hubs. If this still doesn't work, an extra power adaptor is needed.
The drive is performing very slowly	*Is your DiskCrypt Mobile DCM300 connected to a USB 2.0 port?*	To get USB 2.0 Hi-Speed performance, ensure that your DCM300 is connected to a USB 2.0 port.
	Are you using the included DiskCrypt Mobile USB cable?	Only use the included DiskCrypt *Mobile* USB2.0 certified Y-cable. Other USB cables may be of inferior quality.
	Is DiskCrypt Mobile DCM300 plugged into a USB hub?	Connect the DCM300 directly to two USB 2.0 ports on your computer
	Are other USB devices connected to the same port?	Disconnect any other USB devices and see if performance improves.